# WEG IN DIE ZUKUNFT

## DER AUSBLICK IST DIGITALER DENN JE

VON KARIN LEGAT

DER DIGITALE PFAD FÜR PRIVATE UND UNTERNEHMEN IST MITUNTER STEINIG. NICHT NUR IT-SECURITY IST GEFORDERT – AUCH BILDUNG UND GESELLSCHAFT.

**Laut Bundeskriminalamt gibt es kaum eine Kriminalitätsform**, bei der Elektronik, IT und ihre Vernetzung keine Rolle spielen. In Österreich hielt sich die Zahl der Cybercrime-Delikte zwischen 2012 und 2015 bei etwa 10.000, 2016 sprang sie auf 13.100 und 2017 auf 16.800. 2017 wurden laut dem US-Versicherungskonzern American International Group weltweit so viele Stör- und Cyberattacken verzeichnet wie in den vier Jahren davor zusammengenommen. Bei den Angriffen handelt es sich meist um Ransomware, Verschlüsselungstrojaner, die den Datenzugriff oder den gesamten Computer bis zur Lösegeldzahlung lahmlegen. Zuletzt hat auch das Abschöpfen von Kryptowährungen von einzelnen Servern oder Computern zugenommen. In nahezu allen Geräten und Lebensbereichen spielen Computer mittlerweile eine zentrale Rolle. Die Welt ist geprägt von umfassender Digitalisierung und Vernetzung.

»Man muss keine physikalischen Hindernisse überwinden. Mit dem gleichen Effekt kann elegant, mit weniger Kosten und einfacher in jedes System weltweit eingedrungen werden. Alles läuft elektronisch«, benennt Helmut Leopold, Head of Center for Digital Safety & Security am AIT, das große Bedrohungsszenario. Digitalisierung und Vernetzung finden sich nicht nur im IT-Netz eines Unternehmens, vielmehr auch bei Brandmeldeanlagen und Videoüberwachung, Zutrittskontrolle und Sprachalarmierung. Schutz vor Bedrohung durch Internetkriminalität gestaltet sich für Privatpersonen als auch für Unternehmen und Einrichtungen der öffentlichen Verwaltung immer anspruchsvoller. »Das bremst leider das Vertrauen in neue Technologien, die eigentlich viel Potenzial für das Gemeinwohl haben«, betont Harald Leitenmüller, Chief Technology Officer von Microsoft Österreich.

> DIE SICHERSTE IT-INFRASTRUKTUR HILFT NICHTS, WENN DER USER FAHRLÄSSIG HANDELT.

### >> Cybercrime im Vormarsch <<

Die Angriffe werden technisch immer raffinierter. Im Fokus der Angreifer stehen meist große Konzerne und mittelständische Betriebe. Aber nicht nur Banken, Versicherungen oder Fondsgesellschaften müssen sich gut vor Cyber-Attacken schützen. Spätestens seit Inkrafttreten der EU-Datenschutzgrundverordnung sollten auch Berater ihre IT-Systeme aufgerüstet haben. Nicht selten haben es Kriminelle auf hochsensible Daten abgesehen. Verschlüsselungstrojaner werden meist durch E-Mails, unsichere Downloads aus dem Internet sowie Sicherheitslücken in den verwendeten Web-Browsern und Betriebssystemen verbreitet. Ebenfalls auf die Verbreitung durch E-Mails setzen Cyberkriminelle bei Phishing-Attacken.

Die Bekämpfung von Cyberkriminalität und Schaffung sicherer Umgebungen muss deshalb oberste Priorität haben. Für einige Firmen wird das zum Problem. Denn durch die steigende Komplexität von IT-Systemen und immer neue Bedrohungslagen verfügen manche Unternehmen intern nicht mehr über die notwendigen Ressourcen. Sie müssen externe Partner wählen. Die Kosten für »Managed Services« liegen nicht in astronomischen Höhen – je nach Funktionsumfang zwischen zwei und zehn Euro pro Mitarbeiter und Monat. Wichtig ist die regelmäßige Überprüfung, ob die Geschäfts-Unit über die bestmögliche Software für die spezifischen ▶

Die Cyber Range ist eine virtuelle Umgebung des AIT mit online Zugriffsmöglichkeiten für die flexible Simulation kritischer digitaler IT Systeme mit unterschiedlichen Systemkomponenten und Benutzerstrukturen. Ein internationales Team forscht an modernsten Cyber-Security-Technologien, wie Security by Design, neuen Verschlüsselungstechnologien und künstlicher Intelligenz.

## TIPP

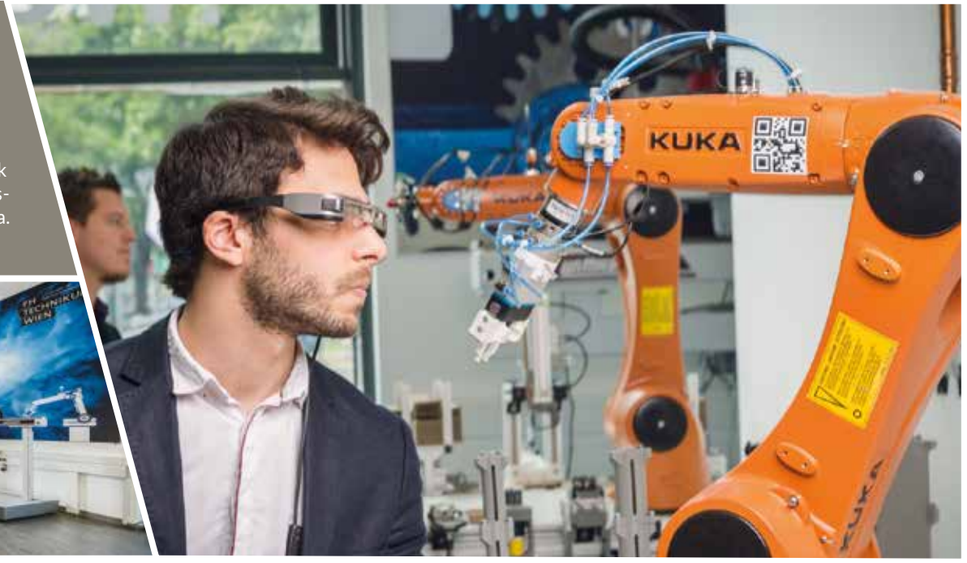
DIE ZAHL DER CYBER-ATTACKEN IST IN DEN LETZTEN JAHREN MASSIV GESTIEGEN. SIEBEN TIPPS, WIE SICH UNTERNEHMEN VOR UNLIEBSAMEN ANGRIFFEN SCHÜTZEN KÖNNEN.

1. Nicht nur das Virenprogramm updaten, sondern auch Software, Betriebssysteme und Firewall.
2. Umfassende Backup-Strategie bereit haben, z.B. gegenseitig überwachende Server-Systeme und tägliche Sicherungen, die offline aufbewahrt werden.
3. Passwortregelungen – Verzicht auf einfache Zahlenkombinationen sowie regelmäßige Änderung.
4. Erstellen einer Desaster-Recovery-Strategie für den Notfall.
5. Entsprechende Zusammenarbeit mit dem Internetdienstanbieter rund um die Überwachung des Datenverkehrs im Backbone.
6. Aufstellen einer Risiko-Analyse und einer Strategie zur Schadensbegrenzung.

*Quelle: Iphos IT Solutions*

In der Digitalen Fabrik der FH Technikum Wien wird ein integriertes Sicherheitskonzept als Pilotprojekt implementiert, validiert und von TÜV Austria zertifiziert. Die Digitale Fabrik ist Living Lab für den Wissenstransfer an Unternehmen, v.a. KMU, und Hochschulen.

Die Maschinensicherheit wird aufgrund des zunehmenden Softwareanteils in der intelligenten Produktion immer stärker von der IT-Sicherheit bestimmt. Maschinensicherheit (Safety) und IT-Sicherheit (Security) sind nicht mehr trennbar. Mit diesen komplexen Wechselwirkungen befasst sich das Forschungsprojekt SIP 4.0 an der FH Technikum Wien.




> MALWARE WIRD SMARTER UND IST IN DER LAGE, SICH INTELLIGENT ANZUPASSEN UND TRADITIONELLE ERKENNUNGS- WIE BESEITIGUNGSROUTINEN ZU UMGEHEN.



Anforderungen des Netzwerks verfügt. Zusätzlich sollten Protokolle aktiv sein, die dafür sorgen, dass diese Software niemals versehentlich deaktiviert wird. Daher ist es ratsam, eine Gruppenrichtlinienkontrolle einzurichten, die Endbenutzer und untergeordnete Administratoren daran hindert, die Anti-Malware-Software zu deaktivieren.

### >> Awareness-Training <<

»Die digitale Transformation verändert jeden Bereich unseres Lebens grundlegend«, betont Harald Leitenmüller. Sieht er auch, dass wir Richtung vorgegebenes Leben steuern, Richtung gesicherter Ablauf? Ganz im Gegenteil: »Ein vorgegebener, strikter Ablauf gehört der Vergangenheit an.« Leitenmüller sieht Cloud Computing als hochflexibles Angebot, welches in der Lage ist, Menschen und Unternehmen in ihrer individuellen und unterschiedlichen Art zu unterstützen, Rechenleistungen an jedem Ort und zu jeder Zeit in Anspruch zu nehmen. Dadurch lässt sich Beschäftigung flexibler an die individuelle Lebenssituation anpassen und wird familiengerechter.

Microsoft investiert jährlich mehrere Milliarden Dollar in die Sicherheit und Weiterentwicklung seiner Cloud-Infrastruktur, die Server werden laufend gegen die neuesten Sicherheitslücken gepatcht.

Helmut Leopold vom AIT weist auf ein generelles Manko hin. »Meine Generation hat die Technik noch hinterfragt und Bedienungsanleitungen gelesen. Die junge Generation, die damit aufwächst, sieht alles als automatisch an. Man drückt einen Knopf und es funktioniert. Sicherheit ist für sie unsichtbar.« Dazu brauche es dringend Awareness-Trainings. In den letzten Jahren sei hier zu wenig getan worden, so der Experte, es gibt vieles nachzuholen. Die sicherste IT-Infrastruktur hilft nichts, wenn der User fahrlässig handelt. Als Aufgabe der Eltern sieht Leopold dieses Aufrütteln nicht. »Ältere Technologien wurden über mehrere Generationen langsam eingeführt, YouTube, Facebook & Co sind über wenige Jahre auf den Markt gekommen. Plötzlich war die gesamte Welt vernetzt.« Es wäre unfair, Eltern in die Verantwortung zu nehmen. Stattdessen müssten Mediengesellschaft, Servicebetreiber, Hersteller und Technologieanbieter agieren und zum Beispiel auch mit dem Schulsystem massiv zusammenarbeiten.

### >> Arbeit an der Sicherheit <<

»In der Sicherheitswelt von morgen sehen wir verstärkt den Einsatz von Machine Learning und Artificial Intelligence zur Unterstützung der Angriffserkennung«, betont Christian Kaufmann, Leiter des Master-Studiengangs IT-Security an der FH Technikum Wien. Die Sicherheit der Zukunft schafft damit neue Jobs, die sich vor allem mit dieser Thematik befassen. Denn der Mensch am Arbeitsplatz wird auch in dieser Branche künftig nötig sein. Kaufmann: »Bislang haben wir keine Silver Bullet im Bereich der Cybersecurity gefunden, auch AI ist definitiv keine.«

Dem herrschenden Expertenmangel steht gegenüber, dass Cybercrime ein Milliardengeschäft mit enormen Zuwachsraten ist. Jeder kann Opfer werden. In den letzten Jahren wurden verstärkt Klein- und Mittelunternehmen angegriffen. Diesen Unternehmen fehlt oft das Budget für die notwendigen Sicherheitsmaßnahmen, sie wiegen sich aber oft in Sicherheit: »Welcher Angreifer hat Interesse an uns Kleinen?« Auch Privatpersonen sind, wie spätestens seit den Ransomware-Angriffen deutlich, ein lukratives Ziel.

Auch die Gegenwehr organisiert sich: Microsoft verweist auf seine Digital Crimes Unit, die bereits vor über zehn Jahren geschaffen wurde. Am AIT wird seit Jahren ein modernes Cyber-Trainingszentrum betrieben, die Cyber Range, in der Schutz- und Abwehrmaßnahmen kritischer IT-Infrastrukturen realitätsnah getestet werden können.

AIT-Manager Leopold fordert, dass das Prinzip Security by Design vorangetrieben wird. »Alles, was wir bauen, ist funktionalitätsgetrieben, besser und schneller. Sicherheit wird als automatisch vorhandener Faktor angesehen und hat bislang keinen Marktwert.« Der Experte ortet das als menschliches Problem. Wenn die Gefahr nicht gesehen wird, warum soll ich mich dagegen schützen? Das betrifft auch die Industrie, die mitunter Sicherheitsmaßnahmen reduziert, wenn sie nicht eingefordert werden. Dort braucht es Standards und Vorgaben wie die NIS-Richtlinie, die EU-Richtlinie zur Sicherheit bei Netz- und Informationssystemen. Neue Zukunftstechnologien wie künstliche Intelligenz und das Internet der Dinge müssen den aktuellen Regeln und Gesetzen für das Sammeln, Nutzen und Speichern von Daten entsprechen. Die NIS-Richtlinie zielt auf Cybersicherheit, gilt für kritische Infrastruktur wie Trinkwasserversorgung, Energie, Finanz und Gesundheit und verlangt technische und organisatorische Maßnahmen zur Sicherung von Netzwerken sowie Informationssystemen und fordert die unverzügliche Benachrichtigung der Behörde bei Cyberattacken und Störfällen. »Der Kommunikationsaustausch muss verbessert werden. Vernetztes Kommunizieren ist nötig, denn kein Land kann die Probleme allein lösen. Kriminalität ist dagegen stets bestens vernetzt«, betont Leopold.

Vor zwei Jahren als Empfehlung veröffentlicht, hatten die EU-Mitgliedstaaten bis Anfang Mai Zeit, die Richtlinie in nationales Recht umzusetzen. Österreich ist säumig, NIS befindet sich nach wie vor in Begutachtung. Dem Vernehmen nach soll die Bundesregierung in den kommenden Wochen ein neues Cybersicherheitsgesetz vorstellen. Details daraus werden noch nicht genannt.

### >> Security-Training <<

»In den klassischen informatiklastigen Bachelorstudiengängen wie Informatik, Wirtschaftsinformatik oder Informations- und Kommunikationssysteme wird das Thema IT Security im Regelstudium behandelt«, betont Christian Kaufmann. Darüber hinaus haben interessierte Studierende die Möglichkeit, ihr Wissen in Wahlpflichtfächern zu vertiefen. Mit dem Master IT-Security schafft die FH Technikum Wien eine fundierte und spezialisierte Ausbildung. Da Security eine komplexe Querschnittsmaterie ist, die viele Bereiche betrifft – von Security Policies für Unternehmen bis zu Ethical Hacking respektive Penetration Tests, von Risikoanalyse bis zur Firewall Konfiguration und System Hardening – bietet der Master IT-Security auch drei unterschiedliche Karrierepfade mit unterschiedlichen Wahlpflichtfächern an. »Jeder, der mit Computern zu tun hat, muss über ein grundlegendes Security-Knowhow verfügen. Die ›Dos and Don'ts‹ sollten bereits in der Sekundarstufe eins Teil des Unterrichts sein. Davon sind wir aber sehr weit entfernt«, bedauert Kaufmann. ■

> Für Helmut Leopold, Head of Center for Digital Safety & Security, ist das Prinzip Security by Design ein Ausweg aus der Sicherheitsproblematik. »Bereits im Software-Entwicklungsprozess müssen Sicherheitsaspekte erheblich stärker beachtet werden. Software ist so unempfindlich als möglich gegen Angriffe zu konzipieren.« Das bedeute zwar einen höheren Aufwand beim Designen, aber im Finish eine höhere Sicherheit.

Foto: FH Technikum Wien/Baumgartner, AIT, Microsoft

> Erhöhte Sicherheitsvorkehrungen werden oft mit Produktivitätshemmungen assoziiert. Harald Leitenmüller widerspricht: »Mit Windows Hello ist das Login am Computer per Fingerabdruck oder ausgeklügelter Gesichts- und Iriserkennung möglich. Die Anmeldung am Rechner dauert weniger als zwei Sekunden. Das ist nicht nur schneller als die herkömmliche Passworteingabe, sondern auch sicherer.«